CLAIMS:

What is claimed is:

1. A method for controlling presentation of a computer readable media of a media storage device, said method comprising:

verifying the presence of a media presentation mechanism and a usage compliance mechanism on a computer system, said usage compliance mechanism comprising a file system filter driver for controlling data reads associated with said computer readable media, said media presentation mechanism communicatively coupled with said usage compliance mechanism;

performing a first decryption of said computer readable media with said file system driver; and

performing a second decryption of said computer readable media and presenting said computer readable media with said media presentation mechanism.

2. The method as recited in Claim 1 further comprising:

installing said usage compliance mechanism on said computer system when said usage compliance mechanism is not present on said computer system; and

installing said media presentation mechanism on said computer system when said media presentation mechanism is not present on said computer system.

3. The method as recited in Claim 2 further comprising:

using an autorun mechanism disposed on said media storage device for initiating said installing of said usage compliance mechanism on said computer system in response to said computer system receiving said media storage device; and

using said autorun mechanism for initiating said installing of said media presentation mechanism on said computer system in response to said computer system receiving said media storage device.

4. The method as recited in Claim 1 further comprising:

affixing a unique identifier to said media storage device.

5. The method as recited in Claim 4 wherein said unique identifier is a serial number and comprising:

generating said serial number before or during disposition of said computer readable media on said media storage device.

6. The method as recited in Claim 5 further comprising:

watermarking said computer readable media via said media presentation mechanism during decryption of a first encryption applied to said computer readable media, said media presentation mechanism further causing said unique identifier to be watermarked onto an outgoing data stream containing said computer readable media.

7. The method as recited in Claim 1 further comprising:

encrypting said computer readable media prior to disposal of said computer readable media on said media storage device.

8. The method as recited in Claim 7 wherein said encrypting comprises:

applying a first encryption to said computer readable media; and

applying a second encryption to said first encryption of said computer readable media.

9. The method as recited in Claim 7 wherein said encrypting comprises:

applying a first unique encryption to each instance of said computer readable media when a plurality of computer readable media is disposed on said media storage device; and

applying a second unique encryption to each said first unique encryption of said computer readable media.

10. The method as recited in Claim 8 further comprising:

decrypting said second encryption with said file system filter driver using a second decryption key stored by said media storage device.

11. The method as recited in Claim 8 further comprising:

decrypting said first encryption with said media presentation mechanism using a first decryption key stored by said media storage device before or concurrent with said presenting.

12. The method as recited in Claim 8 further comprising:

communicatively coupling said computer system with a server; and

decrypting said second encryption with said file system filter driver using a second decryption key stored by said server.

13. The method as recited in Claim 8 further comprising:

communicatively coupling said computer system with a server; and

decrypting said first encryption with said media presentation mechanism using a first decryption key stored by said server.

14. The method as recited in Claim 1 further comprising:

communicatively coupling said computer system with a network;

availing to said network an instance of said computer readable media for sharing among a plurality of nodes of said network by said computer system;

decrypting said instance of said computer readable media from an encryption local to said computer system;

encrypting said instance of said computer readable media into an intermediate encryption; and

transferring said instance of said computer readable media in said intermediate encryption to a node of said network, wherein said decrypting and said encrypting and said transferring are in response to receiving a request for said instance of said computer readable media from said node.

15. The method as recited in Claim 14 further comprising:

receiving an intermediate encryption key by said computer system, said intermediate encryption key for said encrypting said instance of said computer readable media into said intermediate encryption.

16. The method as recited in Claim 15 further comprising:

generating a request by said computer system for said intermediate encryption key; and

receiving said intermediate encryption key from an administrative node of said network.

17. The method as recited in Claim 14 further comprising:

using a client application coupled with said computer system to perform said decrypting and said encrypting.

18. The method as recited in Claim 14 further comprising:

using said media presentation mechanism to perform said availing to said network said instance of said computer readable media.

19. The method as recited in Claim 14 further comprising:

updating said media presentation mechanism and said usage compliance mechanism via said network.

20. The method as recited in Claim 14 further comprising:

storing said instance of said computer readable media in a custom file system of memory coupled with said computer system, said custom file system accessible to a media presentation mechanism.

21. A system for controlling presentation of a computer readable media of a media storage device comprising:

a usage compliance mechanism comprising a file system filter driver for controlling data reads associated with said computer readable media and for performing a second decryption of said computer readable media;

a media presentation mechanism communicatively coupled with said usage compliance mechanism for performing a first decryption of said computer readable media and presenting said computer readable media;

a detecting component for detecting the presence of said usage compliance mechanism and said media presentation mechanism on a computer system; and

an authorizing component for authorizing a recipient of said media storage device to experience said computer readable media provided said usage compliance mechanism is installed on said computer system.

22. The system as recited in Claim 21 further comprising:

an autorun component disposed on said media storage device for automatically installing said usage compliance mechanism when said usage compliance mechanism is not detected on said computer system and for automatically installing said media presentation mechanism when said media presentation mechanism is not detected on said computer system, said autorun

component invoked in response to said computer system receiving said media storage device, said autorun component disposed on said media storage device.

23. The system as recited in Claim 21 further comprising:

an encrypting component for encrypting said computer readable media prior to disposition of said computer readable media on said media storage device, wherein said encrypting comprises a first encryption applied to said computer readable media and a second encryption applied to said first encryption of said computer readable media.

24. The system as recited in Claim 23 wherein said encrypting component applies a first unique encryption to each instance of said computer readable media disposed upon said media storage device and a second unique encryption to each said first unique encryption and associated computer readable media.

25. The system as recited in Claim 23 wherein said file system filter driver comprises:

a first decryption component for decrypting said second encryption with a second decryption key stored by said media storage device.

26. The system as recited in Claim 23 wherein said media presentation mechanism further comprises:

a second decryption component for decrypting said first encryption with a first decryption key stored by said media storage device.

27. The system as recited in Claim 21 further comprising:

an identification component for providing a unique identification for said media storage device, and wherein said unique identification is disposed on said media storage device.

28. The system as recited in Claim 27 wherein said media presentation mechanism further comprises:

a watermarking component for watermarking said computer readable media, and for causing said unique identification to be watermarked onto an outgoing data stream containing said computer readable media.

29. The system as recited in Claim 21 further comprising:

a network communicatively coupled with said computer system, wherein said computer system is configured to transfer an instance of said computer readable media to a node of said network in response to a request from said node, said instance of said computer readable media decrypted from an encryption local to said computer system and encrypted into an intermediate encryption for transfer to said node.

30. The system as recited in Claim 29 further comprising:

a custom file system disposed on memory coupled with said computer system, said custom file system for storing said instance of said computer readable media.

31. The system as recited in Claim 29 further comprising:

a client application configured to request an intermediate encryption key from an administrative node of said network, said intermediate encryption key for enabling said client application to encrypt said instance of said computer readable media into said intermediate encryption.

32. The system as recited in Claim 31, wherein said client application is further configured to decrypt said instance of said computer readable media from said encryption local to said computer system and to encrypt said instance of computer readable media into said intermediate encryption subsequent to receiving said intermediate encryption key.

33. The system as recited in Claim 29 wherein said file system filter driver comprises:

a first decryption component for performing said second decryption with a second decryption key stored on a node of said network.

34. The system as recited in Claim 29 wherein said media presentation mechanism further comprises:

a second decryption component for performing said first decryption with a first decryption key stored on a node of said network.

35. The system as recited in Claim 29 further comprising:

an updating component for updating said usage compliance mechanism and said media presentation mechanism, said updating component communicatively coupled with said computer system and said network.

36. The system as recited in Claim 21 further comprising:

an uninstalling component for automatically removing said usage compliance mechanism and said media presentation mechanism from said computer system when said media storage device is uncoupled from said computer system.

37. A computer readable medium for storing computer implemented instructions, said instructions for causing a computer system to perform a method for controlling presentation of a computer readable media on a media storage device, said method comprising:

verifying the presence of a media presentation mechanism and a usage compliance mechanism on a computer system, said usage compliance mechanism comprising a file system filter driver for controlling data reads associated with said computer readable media, said media presentation mechanism communicatively coupled with said usage compliance mechanism;

performing a first decryption of said computer readable media with said file system filter driver; and

performing a second decryption of said computer readable media and presenting said computer readable media with said media presentation mechanism.

38. The computer readable medium of Claim 37 wherein said method further comprises:

installing said usage compliance mechanism on said computer system when said usage compliance mechanism is not present on said computer system; and

installing said media presentation mechanism on said computer system when said media presentation mechanism is not present on said computer system.

39. The computer readable medium of Claim 38 wherein said method further comprises:

using an autorun mechanism disposed on said media storage device for initiating said installing said usage compliance mechanism on said computer system in response to said computer system receiving said media storage device; and

using said autorun mechanism for initiating said installing said media presentation mechanism on said computer system in response to said computer system receiving said media storage device.

40. The computer readable medium of Claim 37 wherein said method further comprises:

affixing a unique identifier to said media storage device.

41. The computer readable medium of Claim 40 wherein said unique identifier is a serial number generated before or during disposition of said computer readable media on said media storage device.

42. The computer readable medium of Claim 41 wherein said method further comprises:

watermarking said unique identifier onto an outgoing data stream containing said computer readable media using said media presentation mechanism.

43. The computer readable medium of Claim 37 wherein said method further comprises:

encrypting said computer readable media prior to disposal of said computer readable media on said media storage device.

44. The computer readable medium of Claim 43 wherein said encrypting comprises:

a first unique encryption applied to each instance of said computer readable media when a plurality of said computer readable media is disposed on said media storage device, and

a second unique encryption applied to each said first unique encryption and associated computer readable media.

45. The computer readable medium of Claim 43 wherein said encrypting comprises a first encryption applied to said computer readable media and a second encryption applied to said first encryption of said computer readable media.

46. The computer readable medium of Claim 45 wherein said method further comprises:

decrypting said second encryption with said file system filter driver using a second decryption key stored by said media storage device.

47. The computer readable medium of Claim 45 wherein said method further comprises:

decrypting said first encryption with said media presentation mechanism using a first decryption key stored by said media storage device before or concurrent with said presenting.

48. The computer readable medium of Claim 45 wherein said method further comprises:

communicatively coupling said computer system with a server; and

decrypting said second encryption with said file system filter driver using a second decryption key stored by said server.

49. The computer readable medium of Claim 45 wherein said method further comprises:

communicatively coupling said computer system with a server; and

decrypting said first encryption with said media presentation mechanism using a first decryption key stored by said server.

50. The computer readable medium of Claim 37 wherein said method further comprises:

communicatively coupling said computer system with a network;

availing to said network an instance of said computer readable media for sharing among a plurality of nodes of said network by said computer system;

decrypting said instance of said computer readable media from an encryption local to said computer system;

encrypting said instance of said computer readable media into an intermediate encryption; and

transferring said instance of said computer readable media in said intermediate encryption to a node of said network, wherein said decrypting and said encrypting and said transferring are in response to receiving a request for said instance of computer readable media from said node.

51. The computer readable medium of Claim 50 wherein said method further comprises:

receiving by said computer system an intermediate encryption key for said encrypting said instance of said computer readable media into said intermediate encryption.

52. The computer readable medium of Claim 51 wherein said intermediate encryption key is received by said computer system in response to requesting said intermediate encryption key from an administrative node of said network.

53. The computer readable medium of Claim 50 wherein said decrypting and said encrypting are performed by a client application coupled to said computer system.

54. The computer readable medium of Claim 50 wherein said media presentation mechanism performs said availing to said network said instance of said computer readable media.

55. The computer readable medium of Claim 50 wherein said method further comprises:

updating said media presentation mechanism and said usage compliance mechanism via said network.

56. The computer readable medium of Claim 50 wherein said method further comprises:

storing said instance of said computer readable media in a custom file system of memory coupled to said computer system, said custom file system accessible by a media presentation mechanism.